UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/507,190	09/09/2004	Pim Theo Tuyls	NL 020192	1803

24737 7590 05/27/2008
PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER	
TRAORE, FATOUMATA	
ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
05/27/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/507,190	TUYLS ET AL.	
	Examiner	Art Unit	
	FATOUMATA TRAORE	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 March 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4 and 9-20* is/are rejected.

7)☒ Claim(s) *5-8* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the amendment filed March 20, 2008. Claims 17 and 18 have been amended; Claims 1-20 are pending in this application and have been considered below.

Specification

2. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: Claim 9 recites the limitation "readable media ". There is insufficient antecedent basis for this limitation in the claim.

Response to Arguments

3. Applicant's arguments filed 03/20/2008 have been fully considered but they are not persuasive.

4. With regard to the 101 rejection, the 101 rejection of claims 1-20 has been withdrawn in light of applicant argument.

5. With regard to the prior art rejection, Applicant argues that “[n]either Leighton nor Hoffstein teaches or suggests calculating a common secret between two parties as a product of two symmetrical polynomials.” According to Applicant, “the Office action fails to identify which of Hoffstein’s terms are asserted to be a secret that is common to the parties”, “the above text fails to identify any of Hoffstein’s terms as being a symmetrical

polynomials, and specifically does not identify any of the calculated terms as being a product of two symmetrical polynomials." See response at page 9 of 11.

The examiner respectfully disagrees.

Applicant acknowledges that steps 1-4 of Hoffstein's Figure 5 teach the calculation of a polynomial h(x) as the product of two polynomials, g(x) and (f(x) + c(x)). However, Applicant contends that "the applicants respectfully note that nowhere in Hoffstein are the polynomials g(x) and (f(x) + c(x)) taught to be symmetrical polynomials.

It should be noted that a symmetrical polynomial (or algorithm) uses a secret or private key (or value), while an asymmetrical polynomial (or algorithm) uses two keys or values (a public key and a private key). The examiner submits that the polynomials of Hoffstein are symmetrical polynomials.

Hoffstein discloses that the polynomials are private key polynomials. Hoffstein discloses a first polynomial and a second polynomial, wherein the constraints on the polynomials are selected such that an attacker will find it very difficult to recover the private key polynomial from the partial information sent between the prover (first party) and verifier (second party). See abstract.

Leighton and Hoffstein disclose a first party holding a symmetrical polynomial P(x,y) fixed in the first argument by a value p1 and a symmetrical polynomial Q(x,y) fixed in the first argument by a value q1, and sends the values p1 and q1 to a second party. See, for example, Leighton at column 4, lines,55-65 and Hoffstein in figures 1A and 1B. Furthermore, Leighton et al discloses that a pair of users or parties I and j use their individual keys to compute a common secret key. See abstract; column 4, lines 55-65.

It is submitted that the combination of Hoffsteing and Leighton discloses the claimed limitations. Accordingly, the rejection is maintained.

It is also submitted that a prima facie case of obviousness has been established since the combination of Hoffstein and Leighton teaches all the claimed limitations.

To the extent that the response to the applicant's arguments may have mentioned new portions of the prior art references which were not used in the prior office action, this does not constitute new a new ground of rejection. It is clear that the prior art reference is of record and has been considered entirely by applicant. See In re Boyer, 363 F.2d 455, 458 n.2, 150 USPQ 441, 444, n.2 (CCPA 1966) and In re Bush, 296 F.2d 491, 496, 131 USPQ 263, 267 (CCPA 1961).

The mere fact that additional portions of the same reference may have been mentioned or relied upon does not constitute new ground of rejection. In re Meinhardt, 392, F.2d 273, 280, 157 USPQ 270, 275 (CCPA 1968).

In light of the foregoing, the rejections are sustained and this Office action is made final.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> a. A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1, 9-12, 16-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Leighton et al* (US 5519778) in view of Hoffstein et al (US 6076163).

Claims 1, 16, 17, and 19: Leighton et al discloses a method, a system, a device, and a computer program product for of generating a private pair of key for enciphering communication between the users comprising:

A first party and a second party, in which the first party holds a value PI and a symmetrical polynomial P (x,y) fixed in the first argument by the value pl, and the first party performs the steps of sending the value pl to the second party(the individual secret keys allow two users I and j to easily agree on a common secret key Kij namely Kij = F(I, j). Pi and Qi constitute the secret of chip I) (column 4, lines 43-65), receiving a value P2 from the second party and calculating the common secret $1 by evaluating the polynomial P(pl, y) in P2, characterized in that the first party additionally holds a value ql and a symmetrical polynomial Q(x, z) fixed in the first argument by the value ql(this value is computed by user I evaluating the secret polynomial Pi at point j, and it is computed by user j evaluating the secret polynomial at Qj at point I) (column 4, lines 24-31 lines 43-65, column 5 lines 5 lines 14-40 Figs. 1-3), but does not explicitly discloses the steps of sending ql to the second party, receiving a value q2 from the second party and calculating the secret $1 as SI=Q(ql, q2).P(PI, P2). However, Hoffstein et al discloses a secure user identification method, system, device and computer program product, which further discloses a step of sending ql to the second party (Fig. 3), a step of receiving a value 2 from the second party (Fig. 3) and a step of

calculating the secret Sl(column 3, lines 31-46 and Fig. 3). Therefore, it would have been obvious to one having ordinary skills in the art at the time the invention was made to use a challenge response type of authentication in Leighton et al's disclosure. On would have been motivated to do so in order to maintain a secure communication by not allowing eavesdroppers to access critical information.

Claim 9: Leighton et al and Hoffstein et al disclose a method for of generating a private pair of key for enciphering communication between the users as in claim 1 above, and Leighton et al further discloses that the first party and the second party use a non-linear function on the generated secret S1 and S2, respectively, before using it as a secret key in further communications (n fact, the individual secret key assigned by T to user i consists of the two univariate polynomials P.sub.i =P.sub.i (y)=F(i,y) and Q.sub.i =Q.sub.i (x) =F(x,i). P.sub.i and Q.sub.i constitute the secret key of chip I) (column 4, lines 49-55).

Claim 10: Leighton et al and Hoffstein et al disclose a method for of generating a private pair of key for enciphering communication between the users as in claim 9 above, and Hoffstein et al further discloses that a one-way hash function is applied to the generated secrets S1 and S2(the above described user identification technique can be converted to a digital signature technique by the prover applying a one way hash function to Ag(x) to generate a simulated challenge polynomial) (column 3, lines 30-46). Therefore, it would have been obvious to one having ordinary skills in the art at the time the invention was made

to use a hash function in Leighton et al's disclosure. On would have been motivated to do so in order to maintain a secure communication by not allowing eavesdroppers to access critical information.

Claim 11: Leighton et al and Hoffstein et al disclose a method for generating a private pair of key for enciphering communication between the users as in claim 9 above, and Leiflhton et al further discloses that the first party and the second party use a non-linear function on the generated secret S1 and S2, respectively, before using it as a secret key in further communications (n fact, the individual secret key assigned by T to user i consists of the two univariate polynomials P.sub.i =P.sub.i (y)=F(i,y) and Q.sub.i =Q.sub.i (x) =F(x,i). P.sub.i and Q.sub.i constitute the secret key of chip I) (column 4, lines 49-55).

Claim 12: Leighton et al and Hoffstein et al disclose a method for generating a private pair of key for enciphering communication between the users as in claim 1 above, and Hoffstein et al further discloses that a step of verifying that the second party knows the secret S1 (Fig. 3) (column 4, lines 49-55). Therefore, it would have been obvious to one having ordinary skills in the art at the time the invention was made to include a step of verifying that the second party knows the secret key in Leighton et al's disclosure. On would have been motivated to do so in order to authenticate the users.

Claim 18: Leighton et al and Hoffstein et al disclose a system for of generating a private pair of key for enciphering communication between the users as in claim 17 above, and Hoffstein et al further discloses a storage means for storing the

polynomial P and the polynomial Q in the form their respective coefficients (Fig. 2B, item 30). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Leighton et al such as to include a storage means as taught by Hoffstein et al. The motivation of doing so would have been maintaining data integrity.

8. Claims 2, 3, 4, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Leighton et al (US 5519778) in view of Hoffstein et al (US 6076163) in further view of Matyas et al (US 5953420).

Claim 2: Leighton et al and Hoffstein et al disclose a method for generating a private pair of key for enciphering communication between the users as in claim 1 above, while neither of them exclusive discloses a step of generating random numbers. However, Matyas et al discloses a method for establishing an authenticated shared secret value between a pair of users, which further discloses that the first party further performs the steps of obtaining a random number rl (user A generates a secret value Xla using a pseudorandom number generator) (column 6, lines 15-20), calculating .rl. ql (generates a public value Y1 from the secret value Xl as Y1 = G^xl mod p) (column 6 lines 20-25), sending rl .ql to the second party(each party transmits its own public value Y1 to the other party) (column 6, lines 35-38), receiving r2.q2 from the second party and calculating the secret $1 asSl=Q(ql, rl.r2.q2).P (pl, p2) (each party generates a value Z2 from the public value Y2 received from the other party and its own

secret value X2.as Z2 =Y2^x2 mod p) (column 7, lines 33-45). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Leighton et al and Hoffstein et al such as to generate random number in the secret key exchange protocol as taught by Matyas et al. The motivation of doing so would have been against attempts to retrieve the key.

Claim 3: Leighton et al, Hoffstein et al and Matyas et disclose a method for generating a private pair of key for enciphering communication between the users as in claim 2 above, and Matyas et al further discloses that the first party holds the Value ql multiplied by an arbitrarily chosen value r (user A generates a secret value Xla using a pseudorandom number generator) (column 6, lines 15-20), and the product Q (ql, z). P (pl, y) instead of the individual polynomials P (pl, y) and Q (ql, z) (generatesa public value Y1 from the secret value Xl as Y1 = G^xl mod p) (column 6 lines 20-25), and the first party performs the steps of calculating rl .r.ql, sending rl.r.ql to the second party, receiving r2.r.q2 from the second party and calculating the secret S1 as S1= Q (ql, rl.r2.r.q2). P (pl, p2) (each party generates a value Z2 from the public value Y2 received from the other party and its own secret value X2 as Z2 =Y2^x2 mod p) (column 7, lines 33-45). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Leighton et al and Hoffstein et al such as to generate a Secret S1 as taught by Matyas et al. The motivation of doing so would have been against attempts to retrieve the key.

Claims 4, and 20: Leighton et al and Hoffstein et al disclose a method for generating a private pair of key for enciphering communication between the users as in claims 1 and 16 above, while above, while neither of them exclusive discloses a step of generating the secret key S2. However, Matyas et al discloses a method for establishing an authenticated shared secret value between a pair of users, which further discloses that the second party holds a value P2 and a value q2(Fig. 4, item 400), the symmetrical polynomial P(x, y) fixed in the first argument by the value P2, the symmetrical polynomial Q(x, z) fixed in the first argument by the value q2, and the second party performs the steps of sending q2 to the first party(Fig.7 step 706), receiving ql from the first party (Fig. 7, step 708)and calculating a secret S2 as S2=Q(q2, ql)'P(P2, P1), whereby the common secret has been generated if the secret S2 equals the secret S1(each party generates a value Z2 from the public value Y2 received from the other party and its own secret value X2 as Z2 =Y2^x2 mod p) (column 7, lines 33-45). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Leighton et al and Hoffstein et al such as to generate a secret S1 as taught by Matyas et al. The motivation of doing so would have been against attempts to retrieve the key.

9. Claims 13-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Leighton et al (US 5519778) in view of Hoffstein et al (US 6076163) in further view of Menezes et al (handbook of applied Cryptography, ISBN 0-8493-8523-7 1997).

Claim 13:Leighton et al and Hoffstein et al disclose a method for generating a private pair of key for enciphering communication between the users as in claim 12 above, while neither of them explicitly a step of applying a zero knowledge protocol. However, Menezes et al discloses a similar method, which further discloses that the first party subsequently applies a zero-knowledge protocol to verify that the second party knows the secret S1 (The prover claiming to be A selects a random element from pre-defined set as its secret commitment, and from this computes an associated (public) witness. This provides initial randomness for variation from other protocols runs, and essentially defines a set of questions all of which the prove claims to be able to answer, thereby a priori constraining her forthcoming response. By protocol design, only the legitimate party A, with knowledge of A's secret, is truly capable of answering all the questions, and the answer to any one of these provides no information about A's long-term Secret) (pages 409-410, section (IV)). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Leighton et al and Hoffstein et al such as to use a zero-knowledge protocol as taught by Menezes et al. The motivation of doing so would have been providing unconditional security.

Claim 14:Leighton et al and Hoffstein et al disclose a method for generating a private pair of key for enciphering communication between the users as in claim 12 above, while neither of them explicitly a step of applying a commitment- based protocol and Menezes et al discloses a similar method, which further discloses that the first party subsequently applies a commitment-based protocol to verify that the second party knows the secret S1 (*The prover claiming to be A selects a random element from pre-defined set as its secret commitment, and from this computes an associated (public) witness. This provides initial randomness for variation from other protocols runs, and essentially defines a set of questions all of which the prove claims to be able to answer, thereby a priori constraining her forthcoming response. By protocol design, only the legitimate party A, with knowledge of A's secret, is truly capable of answering all the questions, and the answer to any one of these provides no information about A's long-term secret) (pages 409-410, section (IV)*). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Leighton et al and Hoffstein et al such that to use a commitment based protocol as taught by Menezes et al. The motivation of doing so would have been providing unconditional security.

Claim 15: Leighton et al and Hoffstein et al disclose a method for generating a private pair of key for enciphering communication between the users as in claim 14 above, while neither of them explicitly a step of using a symmetric cipher to encrypt a random challenge. However, Menezes et al disclose a similar method

which, further discloses that the second party uses a symmetric cipher to encrypt a random challenge (*b chooses a random r, computes the witness x = h(r) (x demonstrates knowledge of r without disclosing it and computes the challenge e = PA(r, B)) (page 404, section (I))*, and sends the encrypted random challenge to the first party(*B sends the encrypted random challenge to A. A decrypts e to recover r' and B' computes x' = h (r') (page 404, section (I)* and the first party subsequently uses the same symmetric cipher as a commit function to commit himself to a decryption of the encrypted random challenge (*A sends r= r' to B. B succeeds with unilateral entity authentication of A upon verifying) (page 404, section (I))*. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Leighton et al and Hoffstein et al such as to use a symmetric cipher as taught by Menezes et al. The motivation of doing so would have been providing unconditional security.

Allowable Subject Matter

10. Claims 5-8 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

11. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to FATOUMATA TRAORE whose telephone number is (571)270-1685. The examiner can normally be reached on Monday- Friday (every other Friday off) EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571 272 4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

FT
Monday May 19, 2008

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2136